5 eSecurity

5.1 Personal data 12 19

What Personal Data Is

- It is any data that can be used to identify or recognize somebody
- Any data that can be reconstituted so that it does enable an individual to be identified can also be classed as personal data even if it has been de identified, encrypted or pseudonymised
- Examples of personal data is name, address, phone number, location data, ip address, identification card number, etc

Why personal data should be kept confidential

- Data can fall into the wrong hands and be misused
- Individuals who access someone's personal data can retrieve login details and commit identity fraud
- Fraudsters can take a person's banking information and make unauthorized withdrawals and transfer
- People who announce their holidays/when they will be not home on social media can leave themselves open to burglary
- Sharing personal data on social networks such as s likes and dislikes about politics, religion or their current job can hinder future job opportunities
- Criminals can take business information from people and who run their business online and create false email account and fake employee names
- Credit card scams are on the rise when people use their credit cards for online shopping credit card numbers and security codes can be intercepted
- Home insurance or life insurance could be denied if personal information about risky behaviors that person, or their home is posted on social media sites

- Criminal troll websites specifically looking for detailed medical information and use it to gain personal medical attention for themselves or to sell to others, leading to the owners of that information being denied medical attention due to unpaid debt

How personal data can be kept confidential

De-identification

- It is a common strategy when trying to prevent a person's identity from being revealed
- Items of personal data might be removed from a record, such as individuals name

Pseudonymised data

- It is when instead of removing the personal items of data, they are replaced with a temporary ID
- This means that instead of seeing the person's name, you would see an ID which would mean nothing to you
- The problem is that if, somebody can recognize the individual from the rest of the record, they can replace the ID with the individuals name
- However if the data has been amended to make it appear anonymous in such a way it's impossible to recognize an individual, then it's no longer classed as personal data

Encryption

- Scrambling of data to make it unintelligible
- Converts plain text to cypher text which isn't understandable without decrypting it back again to plain text
- Makes data useless if accessed illegally unless decrypted using key

Data Protection Acts

- Data protection acts are rules organizations must stick to in order to protect data
- A number of workers in organizations need to look at the personal data of other individuals as part of their job hence it's important that workers maintain the confidentiality of personal data

- Organization can encourage workers to be aware of their responsibilities
- Workers who deal with confidential information about other individuals have a duty of confidence, they mustn't share or use confidential information except with the permission of the person who gave it
- Works must sign an agreement, which is called confidentiality agreement as it allows to take out a legal injunction preventing them from unauthorized use

Aggregating Information

- A way of preventing individuals from being identified by combining the personal details of a number of people without identifying anybody
- This may not always safeguard details adequately.

Limiting Posting Updates Online

- Insurance companies and most employers tend to do online background checks such as looking at social media profiles
- Personal information that might persuade a prospective employer not to employ an individual shouldn't be posted
- Insurance companies also use the same approach and tend to charge higher monthly payments depending on the type of lifestyle the customer is portraying online and may use this as evidence when deciding not to pay out on a claim

Removal of Geotag

- The photos and videos people take with their smartphones contain information known as meta data, including the time and place where they were taken (geotag)
- If these photos are intercepted, the individuals address or where they work can be discovered
- Smartphones do have software which can be used to either delete the geotag from images or disable them so they are not tagged

Leaving Out Information

- Only filling required data in for example forms such as name and contact number and not providing additional personal data such as email or address if not required
- A person could still be identified if someone is able to put other parts of data together and recognize the person

Keeping Personal Data Secure

There are a number of different precautions that can be taken in order to keep personal data secure. Some of these are described below:

Firewall

- They are designed to prevent unauthorized network access
- Firewalls examine data coming into the network to see if it is allowable
- It examines data packets and breaks them down into smaller pieces of information such as the IP address they came from
- An IP address is a combination of numbers that identifies each computer in a network
- If it is an IP address that isn't allow, the firewall can block that traffic
- It can prevent certain computers from gaining access to the network
- Firewalls don't always prevent hackers from accessing network, the hacker could physically steal a computer that is permitted to access the network
- They can use software which can change the IP address of their computer to one which is acceptable to firewall

Penetration Testing

- Penetration test is when companies employ somebody to deliberately attack their computer network
- They do this so that the authorized hacker will identify the weaknesses in their system security and the company can take measures to improve it is necessary
- It is done to enable the company to secure personal data from illegal hackers who will attempt to gain unauthorized access to the system

Authentication Techniques

- Typing in a **user Id and password** which only the user knows, inserting or swiping a **smart card** which belongs to the user, or using **biometric data** which relates to physical characteristics of the user can be used as means of authenticating an individual
- Biometric involve the user of iris or fingerprint, although they are expensive iris scanners tend to be more effective since the uniqueness of eye prints can be replicated and its scanner don't require as much cleaning as fingerprint scanner which can be affteced by grease and dirt from fingers
- Two factor or multi factor authentication is more preferred since its more secure as it involves the use of multiple authentication techniques, i.e using pin code and debit card to access bank account through ATM

Levels of Access

- Different groups of users can be granted different levels of access to the data on the network which prevents the ability of hackers being able to retrieve personal data
- Often the level of access granted to user is related to their user ID, but some systems enable all users of network to log on to the system
- Allocating different access level to different groups limits the information that the different groups can see and the actions that they are allowed to take
- They then require the use of particular smart card to access certain data
- Example; doctors being able to see only medical records of patient, admin staff being able to out other non-health related information about user such as insurance number, contact details
- Example; owner of social media account restricting access to their personal details on the platform to just friends or friends of friends or making it public for everyone to view

Network Policies

- A set of rules that allow companies to choose who is allowed to access their computer network and control their use of the network once they have gained access
- Workers are required to sign an agreement such as an acceptable use policy which specifies what use is acceptable or not
- They have to agree not to use the network for illegal, unethical or distracting non work related activities such as downloading copyrighted material or spending time on social networking sites to communicate with friends

- It doesn't prevent hackers from gaining access but it does help limit what employees might be tempted to do with the personal data

Software Updates

- Software updates are useful in eliminating bugs and making the software easy to use but they also effective in eliminating security weaknesses
- If weaknesses are present in an operating system, hackers can take advantages of these in order to access the computer system
- It is important for users to install updates as soon as possible in order to limit the amount of time hackers have to find and exploit these weaknesses
- If a system or app is left without updating for a long time, more hackers may become aware of any vulnerabilities and use that information to gain access to personal information stored on the system or app
- Operating system and anti-virus software tend to be the main types of software that need regular updating

Remote Deletion of Cell Phone

- If a device is lost or stolen, the owner can send a command to it using another phone that will completely remove any data such as personal data from it
- Any of the individuals data that isn't backed up on the cloud will be forever lost but the person who stole the phone won't be able to see any of it
- In order to receive the command to erase all the data, the device has to be turned on and connected to the internet
- Anyone who has stolen the phone can also prevent the data from being deleted by simply turning off the phone and removing the sim card and switching it back on
- Not connecting to any wireless network like Bluetooth or Wi-Fi will also prevent the command from reaching
- In order to send the command the app has to be downloaded on to the phone being used to contact the stolen phone
- The app allows the user to get the stolen phone to ring loudly for five minutes just in case it has been mislaid rather than stolen

Preventing the Misuse of Personal Data

Pharming

- Hackers create a fake website which looks like the actual banks website/legitimate-looking website
- It fools the user into thinking they have gone to the correct website
- Hacker installs a piece of malicious software or code on customer's computer through user who downloads it without realizing.
- Software corrupts the Hosts file on the user's computer
- Software adds the URLs of banks and other important and frequently used websites together with IP address of the fake website
- Fraudster redirects genuine website's traffic to own website
- …user is now sending personal details to fraudsters website
- Hacker gains personal information from website when customer enters details
- Hacker uses the acquired information from the website to log on to the users bank accounts for example and is able to make unauthorized purchases or withdraw cash

How to prevent it:

- Using up to date anti-virus software is one way to prevent the downloading of software which changes the hosts file
- Use firewalls to prevent malicious software entering the computer
- Users need to make sure they install the latest software updates
- An up to date browser can cause an alert to be raised that a fake website has been loaded
- Use a trusted, legitimate internet service provider (ISP)
- Digital certificates can be checked to make sure the site is legitimate
- Use trusted DNS servers and ensure the URL begins with HTTPS and has a padlock next to it
- Poor grammar or spelling can also alert user that it may be a fake site
- Avoid using public Wi-Fi systems

Phishing

- It involves the use of email to persuade people to divulge their personal information
- The email may include a website URL inviting the receiver to go to the site

- Emails and websites just looks like an actual organizations email/website but is able to fake website/email
- Clicking on the link takes the target to a fake website
- The email may ask customer to reply with their bank details
- The email usually contains something that demands the target's immediate attention
- Examples include 'we confirm that you have signed up to our service. You will be charged $2 a day unless you cancel your order on this URL…'
- The website then asks the target to enter their personal or financial information

How to prevent it:

- Use of anti-phishing software on a computer connected to the internet which identifies any content which could be interpreted as phishing contained in websites or emails
- It blocks it and issues user a warning about it, can be often found within web browsers or emails software.
- Use of anti-virus and anti-spyware running on a computer and to update it at regular intervals
- Phishing emails often contain grammatical or spelling mistakes that can be looked out for
- Unexpected and suspicious emails should never be opened or any link should be clicked on it if opened
- Personal details are never asked by organizations through emails, hence one should take caution
- Double check URL and email addresses, mentioned in emails to see if it legit
- Most organizations mention that official emails are automated and monitored by bot ' be replying back while phishing emails tend to ask users to reply back with personal information in certain scenarios

Smishing

- It is variation of phishing in which the fraudsters use SMS/text messages rather than mail to send the message
- The main intention is to get the recipient to reveal their personal details
- Fraudsters use text messages to get users to download an attachment which contains malware which in turn feeds personal data from the phone back to the fraudster
- A smishing message often includes a link to the fake website or it can just ask the recipient to simply type in their bank details in reply to the text

- The message usually contains the a link to an email address where they must send this information
- it also asks them to take an immediate action such as changing their bank account PIN to the one mentioned in message
- It can also be a message that tells them they are entitled to a financial reward
- They may include a telephone number in the message that connects to an automated voice response system pretending to be a bank or legit organization

How to prevent it:

- Use of mobile protection software running at all times
- Looking out for spelling or grammatical errors in the messages
- Ignoring message that require immediate action or offer financial reward that too good to be true
- Not interacting with message that ask you to verify activities that you haven't done or aren't aware of, i.e verifying an online purchase
- Opening senders website itself and looking for authentic URL and digital certificate instead of replying to message or download any of its attachment
- not phone any number contained in the text message

Vishing

- Vishing is voice phishing, where phone calls are made in order to get someone to divulge their personal or banking details
- Fraudster claiming to be from the bank can phone customers telling them that their bank account has been accessed by a hacker and they need to change their password and that they will help them do this
- By giving the fraudster their account number and password, they allow them get full access to their account
- They might also leave a message requiring the user to call a certain number when they are free regarding an urgent matter which is actually the fraudsters number
- This number often goes through an answerphone message asking the customer to leave their account number and other personal details
- They may call the user to notify them about the prize they have won and require them to pay for the shipping or handler/redemption fee by asking them to use their credit card number over the phone

- Sometimes the fraudster will ask the customer to hang up and phone the bank to confirm the call, in an effort to try and convince the customer that the call really is from the bank meanwhile the fraudster hasn't disconnected the call.
- They talk the customer through the process of logging on to the banks website and the customer enters their details in order to transfer money to their new account which has been set up by the bank, this is fraudsters own bank account

How to prevent this:

- Calling the bank through helpline number mentioned on their official social media pages and online or on the credit/debit card and confirming if a call was made by them
- Not to share personal details on the call even when they ask for it or when they mention the call is on hold and it's not being recorded
- Blocking the number
- Users should register their phone with the 'national do not call registry'
- Don't call a number mentioned in a voice mall
- Don't answer phone calls from number you don't recognize
- Downloading a vishing number app, which filters/blocks numbers that are registered to be spam or fake calls

5.2 Malware

Malware is short for malicious software; it's any program which has been created with the deliberate intention of causing damage or disruption or gaining access to a computer without owner's permission

Trojan Horse

- It is a malicious computer program which is used to hack into a computer and misleads users of its true intent
- It does this by disguising itself as authentic software and enables the person who created it to take control of the computer it has infected
- Trojans generally don't attempt to infect other file and neither do they attempt to self-replicate
- They have to be activated by the attacker

- Trojans can provide a backdoor into your computer so a third party can take control
- They are also able to copy and delete files from the hard disk and can corrupt data
- They can used to be download other malware

Virus

- A type of malware that is designed to spread from one computer to another usually by the means of the internet causing changes in the way each computer operates as it spreads
- They have the ability to replicate themselves
- Viruses can delete the data on disk or corrupt or change the data
- They insert themselves to another computer program and often lie dormant until a situation arises which causes the computer to execute its code
- Symptoms that can indicate a virus are popup windows that suddenly stat appearing frequently, the users homepage being changed so that it is different from what it is normally or their password getting changed, preventing user from being able to log on
- Viruses can cause large numbers of emails to be from the users email account
- The computer may frequently crash or its processing speed can noticeably slow down

Worms

- It is a standalone malicious computer program or code that replicates itself in order to spread to other computers
- A worm exploits security holes in networks and computers in order to spread throughout the network
- It doesn't need to attach itself to an existing program or file so they are standalone programs
- Worms consume bandwidth, slowing down the traffic in a network
- Worms consume processing power, therefore slowing down computer operations
- They can replicate themselves occupying more space
- Can modify or delete file, they are also able to install backdoors
- File going missing or suddenly appearing is an indication of a worm being present

Spyware

- Spyware is a type of malware that collects information about a computer users activities without their knowledge
- A key logger is usually used to collect a record of the users keystrokes, this data is sent to the hacker
- This data could be users personal data such as credit cards number, usernames and passwords
- Spyware also collects data such a web browsing habits
- Spyware doesn't replicate itself like a worm or virus
- A user might notice spyware as it tends to slow down the processing power and bandwidth of their computer and network since these are used by the spyware to communicate information back to hacker

Adware

- It is a malicious software that automatically generates advertisement in order to gain revenue for its author
- It is normally downloaded with free software without the users knowledge
- When the software is opened, these advertisements may appear in the user interfaces or the screen shown to the user by the software
- It examines which internet sites are visited and presents advertising according to the types of goods and services the user in interested in.
- It often causes unrequested advertisement to be displayed in the browser when a user accesses he internet, these could be in popups
- It's more of nuisance than dangerous but in recent days it has been linked to spyware
- Symptoms can be unnoticeable but some types of adware may slow down the performance of a computer and there tends to be larger number of popups than usual

Rootkit

- It is a software designed to provide continued administrator access to a computer while actively hiding it's presence
- Root refers to the Admin account on Unix and Linux systems and kit refers to the software components that implement the tool
- Rootkits can be installed in a number of ways, including phishing attacks or social engineering to trick users into giving the rootkit permission to be installed

- A rootkit allows someone to maintain command and control over a computer without the computer user knowing it
- The controller of the rootkit can remotely execute files and change system configurations on the host machine
- A rootkit can access log files and spy on the computer owners usage
- They are difficult to detect because they are activated before a computers operating system has completely booted up

Malicious Bots

- Bots often automate tasks and provide information or services that would otherwise be conducted by humans
- They are used gather information automatically with instant messaging and other web interfaces
- They may also be used to interact dynamically with websites
- A malicious bot is self-propagating malware designed to infect a host and connect back to a central server or servers
- Attackers can launch broad-based, 'remote-control', 'flood type' attacks against their targets
- They have the worm like ability to self-propagate
- Bots can include the ability to log key strokes, gather password and capture and analyze packets
- They can also launch DDoS attack and open back doors on infected network
- They infect network in a way that escapes immediate notice

Ransomware

- Ransomware is a malicious software that threatens to publish the victims data or block access to it unless a ransom is paid
- It encrypts the victims file making them unpredictable and demands a ransom payment to decrypt them
- It often infiltrates a PC as a computer worm or Trojan horse
- Most ransomware attacks are the result of clicking on an infected email attachment or visiting compromised websites
- Some ransomware allows use of the computer but prevents the opening of certain files

Fileless Malware

- It is a type of malware that doesn't rely on files and leaves no evidence once it has been executed
- It is very difficult or anti-malware software to detect and remove
- It only resides in the main memory (RAM)
- Fileless malware doesn't perform any actions which affect the computer's hard drive
- It ceases to work once the system is rebooted

Scareware

- It is a type of malware that tricks the computer user into thinking that their computer has been infected with a virus
- It appears as a popup and seems to come from a genuine anti-virus provider
- The user then pays the 'provider' to download the anti-virus and then discovers, too late that it's a scam.

How Malware Is Used:

Fraud

- Involves using a computer to take or alter electronic data or gain unlawful use of computer or system to illegally benefit financially
- Spyware is used in fraud as it collects a user's personal data, browsing habits and keystrokes.
- This can lead to credit card fraud as well as identity theft
- Once fraudsters have gained a users' personal and financial data, they can either sell the information to other criminals or they can impersonate the user
- They can use the users financial data to ask the bank for a new PIN or even an extra card
- They can buy goods via the internet using the credit card details they have obtained.
- They can buy goods via the internet using the credit card details they have obtained
- They can also withdraw large sums of money from the user's bank account
- Most credit card fraud victims are unaware of what has happened until it is late
- Scareware is used to obtain money under false pretences
- Phishing, vishing, smishing and pharming are intended to get the user to divulge their passwords, credit card numbers and bank account information so that the fraudster can

access the users account to withdraw money, make money transfer or use the details to shop over the internet

- Ransomware is used to blackmail users into paying large sums of money, usually using Bitcoin so that it can't be traced, the attackers usually pretend to be a cop or an official authority

Industrial Espionage

- malware is used with the purpose of stealing information in the form of company secrets
- Malware can be downloaded without realizing when an employee clicks on adware for example
- Spyware/Trojan is an example of malware that can be used to collect the data and send it back to the hacker
- Malware can be used to gain access to computers, networks or database to get files and secrets such as intellectual property, research projects and future business plans
- Malware is used to exploit weaknesses in software to gain access to the data
- Types of spyware target specific computers for industrial espionage to spy on a particular company

Sabotage

- It refers to making deliberate attacks which are intended to cause computers or networks to cease to function properly
- Computer sabotage within organization is carried out by disgruntled employees intent on causing the organization to lose money
- Employees might make unauthorized attempts to view, disclose, retrieve, delete or change information by misusing he system privileges they have been granted
- Some acts of sabotage are committed by former employees, perhaps happy with the way they lost their job, although most attacks by employees or former employees are carried out remotely
- It can consist of a virus being sent to a computer which prevents users from logging on or in the form of distributing malware to allow hackers to illegally access an organization's network

- Organizations should take measures to protect both hardware and software this could be done using a firewall and anti-virus software, along with regular updates of each individual employee's computer passwords

Consequences for Organizations and Individuals

- The procedures an organization uses to secure its computer network and systems can be wrecked
- It can disturb their business operations leading to for example loss of income
- Hackers can use malware to corrupt, destroy or steal organizations data
- Stolen or leaded data can provide a competitive advantage to their competitors
- Hackers can obtain personal information of employees and clients from organizations leading to legal action and fines being charged against them
- Stolen data can be used to blackmail organizations
- Ransomware can be used to hold organizations to ransom
- Infected computers have to be disconnected from the network so other devices are not infected and fewer machines are available
- Infected computers have to be treated with anti-virus software
- Costs to an organization will increase and extra expertise may need to be brought in to clean computers
- It undermines the confidence in the organization leading to loss of customers and business
- There will also be a great impact of computer and network performance as malware tend to slow down processing speed and decrease bandwidth
- Rootkit allows the computer to be taken over and commit illegal acts
- Stolen data can be auctioned on dark web to the highest bidder

Consequences for Individuals

- Malware enables hackers to gain valuable information such as bank details, date of birth, email address and passwords
- The hacker can then commit identity fraud
- Scareware can be used to fool users into paying for non-existent anti-virus software

- The slowing down of their computer system can be inconvenient to say the least for an individual
- Pranksters may simply want to see the havoc their programs can cause, whereas some hackers would attack PCs with malware to make their reputations within the hacker world

Prevention of Malware:

Use of prevention software

- Anti-virus software must ensure all data is scanned for malicious code as it enters the company's network
- Anti virus can remove virus and alert the user to take action such as deleting infected files or cleaning them
- A firewall, which filters incoming traffic and prevents malicious software entering the system should be used on all the external entry points to the network
- Anti-virus software must be kept up to date, running all the time, with scans scheduled to run at frequent intervals
- Only one anti-virus program should run at a time as two different programs may conflict with each other
- Anti-spyware software should be run if it isn't included in the anti-virus software but it shouldn't conflict with the anti-virus software
- Make use of a spam filter to minimize the effect of spam, especially if an email software doesn't have one
- Anti-malware can be used to protect network computers from the entry of malware in the network and remove malware which managed to get into the computer network system

Physical methods of prevention

- A record should be kept of any known malicious websites which should tehn be blocked by firewall from accessing the network
- Dedicated stand alone virus checking computers which are equipped with anti-virus software should be provided, these must be capable of scanning any type of media

- All employees should be educated to understand the risks from malware and be aware of the day to day procedures they can follow to help prevent malware infections
- They should be encouraged to stop and think before clicking on links, if they encounter a malicious link, they should contact the IT department as soon as possible
- They must not connect any removable media or personally owned device to the network
- They need to be aware that they must report any strange or unexpected system behavior to a technician or ember of the IT department
- Operating systems and browser software should always be kept up to date
- Software that is no longer used or outdated should be removed as they are open to malware attacks
- Emails should be read with suspicion, since encouraging the user to download malware works if sufficient attention is paid to who sent the email and what it might be suggesting
- Look out for incorrect spellings and poor grammar in the message/content as well as the senders address and URL provided
- Strong passwords should be used that are unique and changed often and not related to one's personal information
- Websites should have an appropriate padlock next to the URL
- Users should log off from their computers at the end of a session